APROBAT
proces-verbal al şedinţei Senatului
USMF „Nicolae Testemiţanu"
nr. 2/17 din 26.02.2026

REGULAMENT
privind supravegherea prin mijloace video
și reglementarea accesului în edificii prin terminale de control acces în cadrul
IP Universitatea de Stat de Medicină și Farmacie „Nicolae Testemițanu" din Republica Moldova

I. DISPOZIȚII GENERALE

1. Prezentul Regulament stabileşte cadrul juridic, organizatoric și tehnic privind implementarea, administrarea şi utilizarea sistemului de supraveghere prin mijloace video şi a sistemului de control al accesului în edificiile IP Universitatea de Stat de Medicină și Farmacie „Nicolae Testemițanu" din Republica Moldova (în continuare – Universitatea).

2. În contextul actual, securitatea persoanelor, a patrimoniului și a activităților desfășurate în cadrul Universității nu poate fi asigurată fără un sistem eficient de supraveghere video, care să permită atât monitorizarea în timp real a evenimentelor și persoanelor, cât și înregistrarea imaginilor video în vederea prevenirii și investigării eventualelor incidente.

3. Sistemele de supraveghere video se aplică, în principal, spațiilor aflate în gestiunea Universității, inclusiv:

- ✓ blocuri didactice;
- ✓ cămine studențești;
- ✓ complexe socioculturale;
- ✓ clinici universitare;
- ✓ blocuri și terenuri sportive;
- ✓ spații administrative;
- ✓ parcări și alte spații adiacente.

✓ **4.** Prezentul Regulament este elaborat în temeiul Legii privind protecția datelor cu caracter personal nr. 133 din 08.07.2011, Codului muncii al Republicii Moldova; Cartei Universitare; Regulamentului intern al Universității, altor acte normative în vigoare.

5. Universitatea are calitatea de operator de date cu caracter personal pentru datele colectate prin sistemul de supraveghere video și sistemul de control acces.

6. Prevederile prezentului Regulament sunt obligatorii pentru:

- ✓ personalul universitar;
- ✓ studenți, masteranzi, doctoranzi, medici rezidenți, medici cursanți și alți beneficiari ai procesului de instruire;
- ✓ persoane care prestează servicii în cadrul Universității;
- ✓ vizitatori.

II. SCOPUL SUPRAVEGHERII PRIN MIJLOACE VIDEO

7. Sistemul de supraveghere video este implementat în următoarele scopuri legitime:

a) asigurarea securității persoanelor aflate în incinta Universității;
b) protecția patrimoniului Universității;
c) prevenirea, constatarea și documentarea faptelor ilicite sau alte acțiuni care ontravin regulilor interne ale Univerității;
d) gestionarea situațiilor de urgență;
e) sprijinirea activității structurilor de securitate și pază;
f) respectarea obligațiilor legale în domeniul protecției datelor cu caracter personal;
g) protejarea vieții private, a intereselor legitime și a drepturilor fundamentale ale persoanelor vizate.

8. Supravegherea video se realizează cu respectarea principiilor:
- ✓legalității;
- ✓proporționalității;
- ✓minimizării datelor;
- ✓limitării scopului;
- ✓exactității;
- ✓integrității și confidențialității.

III. ZONELE SUPRAVEGHEATE

9. Camerele de supraveghere sunt amplasate în locuri vizibile, astfel încât persoanele să fie informate despre existența acestora.
10. Este interzisă utilizarea camerelor ascunse sau a altor mijloace de supraveghere clandestină, cu excepția cazurilor expres prevăzute de lege.
11. Nu sunt monitorizate zonele în care persoanele pot avea o așteptare rezonabilă de viață privată, cum ar fi:
- ✓toalete;
- ✓vestiare;
- ✓cabine de duș;
- ✓alte spații similare.

12. Amplasarea camerelor de supraveghere este decisă de către Departamentul Administrarea patrimnoniului și secția Secția de monitorizare video și control acces, care duce evidența locațiilor unde sunt instalate camerele video.

IV. DATELE CU CARACTER PERSONAL COLECTATE

13. Sistemul de supraveghere video funcționează permanent (24/24 ore) și este dotat cu detector de mișcare.
14. Datele colectate constau în imagini video ale persoanelor aflate în zonele supravegheate și, după caz, alte date generate automat de sistem (data, ora, locația).
15. La punerea în funcțiune a sistemului, persoanele împuternicite primesc instructaj privind:
- ✓setările tehnice ale sistemului;
- ✓regimul de confidențialitate;
- ✓procedura de acces la înregistrări;
- ✓responsabilitățile ce decurg din Legea privind protecția datelor cu caracter personal nr. 133 din 08.07.2011.

V. PRINCIPII DE ORGANIZARE ȘI FUNCȚIONARE A SISTEMULUI DE CONTROL ACCES

16. Accesul în edificiile universitare este permis exclusiv prin punctele de control acces dotate cu:
- ✓personal de serviciu;
- ✓terminale de control acces;
- ✓sisteme de supraveghere video.

17. Accesul se realizează prin:
- ✓recunoaștere facială;
- ✓cod PIN;
- ✓card de acces nominal;
- ✓acte de identitate;
- ✓permis nominal;
- ✓carnet de beneficiar de studii.

18. Datele colectate prin sistemul de control acces sunt înregistrate în baza de date a sistemului informațional al Universității.
19. Accesul vizitatorilor în cămine este permis doar însoțiți de locatar, care își asumă responsabilitatea pentru comportamentul acestora.

20. Accesul vizitatorilor în blocurile de studii și laboratoare se efectuează doar însoțiți de personal autorizat.
21. Coordonarea generală a activității sistemului de control acces revine Departamentului Administrarea Patrimoniului.
22. Emiterea și administrarea permisiunilor de acces este în competența Secției Monitorizare Video și Control Acces.
23. Cardurile de acces se eliberează sub semnătură și se utilizează exclusiv în scop personal.
24. Pierderea cardului se notifică în termen de 24 de ore.
25. Reemiterea cardului se face la cerere, cu suportarea costurilor de către titular.
26. La încetarea raporturilor juridice cu Universitatea, cardul se restituie obligatoriu.

VII. ACCESUL LA DATE ȘI DEZVĂLUIREA ACESTORA

27. Accesul la imaginile video este limitat la persoanele desemnate prin ordin al rectorului Universității.
28. Vizualizarea, copierea sau transmiterea înregistrărilor se face numai cu acordul scris al rectorului sau a persoanei desemnate.
29. Dezvăluirea către organele de drept se realizează exclusiv în baza unei solicitări scrise și motivate.
30. Fiecare caz de dezvăluire se consemnează într-un Registru special de evidență.

VIII. MĂSURI TEHNICE ȘI ORGANIZATORICE

31. Universitatea aplică următoarele măsuri:
✓securizarea fizică a serverelor;
✓utilizarea surselor autonome de alimentare (UPS);
✓protecție firewall;
✓parole individuale;
✓actualizarea listei persoanelor cu acces;
✓instruirea periodică a personalului;
✓semnarea acordurilor de confidențialitate

IX. DURATA PĂSTRĂRII ÎNREGISTRĂRILOR

32. Înregistrările video se păstrează timp de 30 de zile calendaristice, după care sunt șterse automat.
33. În caz de incident de securitate, termenul poate fi prelungit până la finalizarea investigației.

X. DREPTURILE PERSOANELOR VIZATE

✓**34.** Persoanele vizate beneficiază de drepturile prevăzute de Legea privind protecția datelor cu caracter personal nr. 133 din 08.07.2011.
✓dreptul de acces;
✓dreptul de rectificare;
✓dreptul de opoziție;
✓dreptul de ștergere.
35. Cererile se soluționează în termen de 15 zile calendaristice.
36. Furnizarea imaginilor se face cu protejarea drepturilor terților prin anonimizare sau estompare.

XI. AUDITUL SECURITĂȚII SISTEMULUI

37. Sistemul păstrează jurnale de acces și activitate.
38. Auditul securității are scopul de a:
- ✓ asigura trasabilitatea acțiunilor;
- ✓ identifica incidente;
- ✓ preveni accesul neautorizat;
- ✓ detecta disfuncționalități tehnice.

XII. INFORMAREA PUBLICULUI

39. Informarea se realizează prin pictograme și note informative amplasate în zonele supravegheate.
40. Universitatea garantează respectarea drepturilor persoanelor vizate şi aplicarea măsurilor legale de protecție a datelor.

XIII. DISPOZIȚII FINALE

41. Regulamentul se completează și se modifică ori de câte ori intervin schimbări legislative.
42. Prezentul Regulament intră în vigoare la data aprobării de către Senatul Universității.